UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/507,191	02/18/2000	Paul England	MS1-408US	8393

22801 7590 12/12/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 12/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/507,191
Filing Date: February 18, 2000
Appellant(s): ENGLAND, PAUL

Rich Bucher
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/12/2006 appealing from the Office action mailed 5/23/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

> The summary of claimed subject matter contained in the brief is deficient. 37 CFR 41.37(c)(1)(v) requires the summary of claimed subject matter to include: (1) a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number, and to the drawing, if any, by reference characters and (2) for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function as permitted by 35 U.S.C. 112, sixth paragraph, must be identified and the structure, material, or acts described in the specification as corresponding to each claimed function must be set forth with reference to the specification by page and line number, and to the drawing, if any, by reference characters.

The brief is deficient because the citations provided by Appellant does not disclose retrieving a plurality of blocks of data from a storage medium wherein at least one block of data includes data not contained in a given content. None of the passages nor the drawings discussed one block of data from the retrieved blocks of data not contained in the given content. Note that

figures 2 and 5, cited by Appellant, show that only one block of data is selected and only if additional verification is required that another block is selected.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,367,019	ANSELL ET AL.	4-2002
5,745,678	HERZBERG ET AL.	4-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 43, and 45-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,367,019 to Ansell et al in view of US Patent 5,745,678 to Herzberg et al. This rejection is set forth in a prior Office Action mailed on 5/23/2006.

As per claim 43, Ansell et al substantially discloses a method comprising: retrieving plurality of data such as retrieving read-only serial number from storage media (see column 8, lines 19-20, retrieving keys from storage 506A1-4, and retrieving component keys which are (shared key of read-only key 504) stored in the player (see column 8, lines 31-43), these data may also be stored in a smartcard (column 13, lines 45-47) that meets the recitation of *retrieving plurality of blocks of data from a storage medium*; and discloses wherein at least one block of data (keys) include data not in a given content (SPT 116) (by retrieving different sets of data

from different fields, the data are not contained in the same content) that meets the recitation of *wherein at least one block of data includes data* (keys) *not contained in a given content* (SPT 116) (see column 6, lines 50-53 and see figure 5, player 150); *generating a digest value for each of the plurality of randomly retrieved blocks of data* (keys and component keys) (see column 8, lines 45-50 and column 7, lines 48-64); *comparing each of the digest values to a set of verification data* (column 8, lines 45-57), *determining that the computer-readable media contains an original version of the given content if the digest values match a subset of the verification data* (data in the identification fields, figure 4) (see column 8, lines 45-65). As interpreted by the Examiner, **Ansell et al** discloses allowing access to a smaller number of times of playback (see column 11, lines 26-38) or allowing access to a selected track of SPT (see column 13, lines 11-15 and column 9, lines 5-13), which meets the recitation of a smaller functionally equivalent version than the original version. **Ansell et al** further discloses allowing access to an encrypted compression version (see column 8, lines 63-67) which is smaller than the original based on the matching of digests values to a subset of verification data (see column 8, lines 45-67) that meets the recitation of *allowing access of a functionally equivalent version of the given content which is smaller than the original version if the digests values match a subset of verification data* (see also column 5, lines 1-18); access to a compressed version which is smaller than the original such as an MP3 format is very well known in the art as disclosed in the background of **Ansell et al** (see column 1, lines 12-20) the invention can also be used to acquire music products from the Internet (see column 13, line 62 through column 14, line 12), therefore, as shown above allowing access to "smaller than the original version" is disclosed. **Ansell et al.** teaches binding content and media identification by generating a digest value for each of a

plurality or set of blocks of data (keys and component keys) retrieved from a storage medium but is silent about the word randomly when teaches retrieving data. However, **Herzberg et al.** in an analogous art teaches protecting multimedia title or program (content) by *randomly retrieving a plurality of blocks of data from a removable medium* (CD ROM) to determine if the content is valid (see column 7, lines 11-18 and column 5, lines 58-60 and column 2, lines 9-14), the random selection helps reduce the possibility of forgery, and processing time, (see column 12, lines 26-32). **Herzberg et al** further discloses *generating a digest value for each of the plurality of randomly retrieved blocks of data* (see column 2, lines 17-21) *comparing each of the digest values* (hash values) *to a set of verification data determining if the digest values* (hash values) *match a subset of the verification data and allowing access if the digests values* (hash values) *match a subset of verification data* (see column 2, lines 20-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Ansell et al** with **Herzberg et al** to include the features of randomly retrieving/selecting when retrieving/selecting a plurality or set of blocks of data to be validated by generating a hash (digest) value for each of the plurality of randomly retrieved blocks of data and comparing hash values (digest) of the plurality or set of data portions of the content as taught by **Herzberg et al** above in order to more efficiently validate the multimedia program because the random selection helps reduce the possibility of forgery and processing time as the checking may be based on only portion of the data (see **Herzberg et al**, column 6, lines 18-39 and column 12, lines 26-32). This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestions provided above by **Herzberg et al.** so as to more efficiently validate the multimedia program to reduce the possibility of forgery, the

motivation to do so is provided by Herzberg who teaches the advantage of checking only a selected portion of the data to be validated rather than checking all of the data *(see column 6, lines 18-34)* in order to minimize the required processing time, *(column 12, lines 26-32)*. As indicated above, checking a small portion of data could be exposed to forgery, thus the invention as taught by Herzberg provides a degree of randomness, "by randomly selecting the portion of data to be validated, the possibility of forgery can be greatly reduced" (see column 6, lines 18-34).

As per claim 45, the combination of **Ansell et al.** and **Herzberg et al** discloses *allowing access to related material if the digest values match a subset of the verification data* (see **Ansell et al**, column 8, lines 45-67 for allowing access to a decrypted version of the key that meets the recitation of related material); (see also **Ansell et al**, column 5, lines 1-18 for allowing access to SPT 116 from tracks 112 or different forms of data (images, video, computer software) that also meets the recitation of related material).

As per claim 50, claim 50 recites similar limitations to claim 43 except for including "receiving a request" and for replacing "allowing access" by "controlling access". **Ansell et al** substantially discloses a method comprising: *receiving a request to access a given content* (SPT) (see column 2, lines 52-67); retrieving keys from storage 506A1-4, and retrieving component keys which are (shared key of read-only key 504) stored in the player (see column 8, lines 31-43), these data may also be stored in a smartcard (column 13, lines 45-47) that meets the recitation of *retrieving set of blocks of data from a storage medium*; and discloses wherein at

least one block of data (keys) include data not in a given content (SPT 116) (by retrieving different sets of data from different fields, the data are not contained in the same content) that meets the recitation of *wherein at least one block of data includes data* (keys) *not contained in a given content* (SPT 116) (see column 6, lines 50-53 and see figure 5, player 150); *calculating a digest value for each of the plurality of randomly retrieved blocks of data* (keys and component keys) (see column 8, lines 45-50 and column 7, lines 48-64); *verifying whether the received* (or retrieved) *plurality of blocks* (keys and component keys) *are from an original version of the given content by comparing the calculated digest values to a set of associated verification digest values* (MAC fields, col 6, lines 59-65), (see column 8, lines 45-57). As interpreted by the Examiner, **Ansell et al** discloses allowing access to a smaller number of times of playback (see column 11, lines 26-38) or allowing access to a selected track of SPT (see column 13, lines 11-15 and column 9, lines 5-13), which meets the recitation of a smaller functionally equivalent version than the original version. **Ansell et al** further discloses allowing access to an encrypted compression version (see column 8, lines 63-67) which is smaller than the original based on the matching of digests values to a subset of verification data (see column 8, lines 45-67) that meets the recitation of *controlling access to a functionally equivalent version of the given content which is smaller than the original version if the digests values match a subset of verification data* (see also column 5, lines 1-18); access to a compressed version which is smaller than the original such as an MP3 format is very well known in the art as disclosed in the background of **Ansell et al** (see column 1, lines 12-20) the invention can also be used to acquire music products from the Internet (see column 13, line 62 through column 14, line 12), therefore, as shown above allowing access to "smaller than the original version" is disclosed. **Ansell et al.** teaches binding content

and media identification by generating a digest value for each of a plurality or set of blocks of data (keys and component keys) retrieved from a storage medium but is silent about the word randomly when teaches retrieving data. However, **Herzberg et al.** in an analogous art teaches protecting multimedia title or program (content) by *randomly retrieving a plurality of blocks of data from a removable medium* (CD ROM) to determine if the content is valid (see column 7, lines 11-18 and column 5, lines 58-60 and column 2, lines 9-14), the random selection helps reduce the possibility of forgery, and processing time, (see column 12, lines 26-32). **Herzberg et al** further discloses *calculating a digest value for each of the plurality of randomly retrieved blocks of data* (see column 2, lines 17-21) *comparing the calculated digest values* (hash values) *to a set of associated verification digest values* (hash values) *and controlling access if the calculated digests values* (hash values) *match a subset of associated verification digest values* (hash values) (see column 2, lines 20-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Ansell et al** with **Herzberg et al** to include the features of randomly retrieving/selecting when retrieving/selecting a plurality or set of blocks of data to be validated by generating a hash (digest) value for each of the plurality of randomly retrieved blocks of data and comparing hash values (digest) of the plurality or set of data portions of the content as taught by **Herzberg et al** above in order to more efficiently validate the multimedia program because the random selection helps reduce the possibility of forgery and processing time as the checking may be based on only portion of the data (see **Herzberg et al**, column 6, lines 18-39 and column 12, lines 26-32). This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestions provided above by **Herzberg et al.** so as to more efficiently

validate the multimedia program to reduce the possibility of forgery, the motivation to do so is provided by Herzberg who teaches the advantage of checking only a selected portion of the data to be validated rather than checking all of the data *(see column 6, lines 18-34)* in order to minimize the required processing time, *(column 12, lines 26-32)*. As indicated above, checking a small portion of data could be exposed to forgery, thus the invention as taught by Herzberg provides a degree of randomness, "by randomly selecting the portion of data to be validated, the possibility of forgery can be greatly reduced" (see column 6, lines 18-34).

As per claim 54, the combination of **Ansell et al.** and **Herzberg et al** discloses the claimed method of claim 50. **Herzberg et al.** further discloses *wherein the set of associated verification digest values* (hash values in validation structure) are stored with the original version of the given content (in the multimedia program) (see column 2, lines 4-7 and lines 17-21). Claim 54 is rejected on the same rationale as the rejection of claim 43.

As per claim 58, claim 58 recites similar limitations to claim 50 except for deleting the step of calculating and for implementing the claimed method of claim 50 into a system comprising: *a data reading device to read data from a computer-readable medium and a verification module coupled to the data reading device.* **Ansell et al** substantially discloses a data reading device (see player 110, 150, 150B, processor 102 in figures 1 and 5) adapted to read data from own storage medium and also by interfacing with each other; and a verification module (502A, 502B, 512A, 512B in figure 5) *adapted to receive a request to access a given content* (SPT) *to request a random set of blocks of data* (see column 9, lines 5-22 and column 10, lines 9-

16); retrieving keys from storage 506A1-4, and retrieving component keys which are (shared key of read-only key 504) stored in the player (see column 8, lines 31-43), these data may also be stored in a smartcard (column 13, lines 45-47) that meets the recitation of *retrieving set of blocks of data from a storage medium*; and discloses wherein at least one block of data (keys) include data not in a given content (SPT 116) that meets the recitation of *that includes at least one block of data* (keys) *that does not contain the given content* (SPT 116) (see column 6, lines 50-53 and see figure 5, player 150); *verifying whether the received* (or retrieved) *plurality of blocks* (keys and component keys) *are from an original version of the given content by comparing digest values* (keys and component keys) (see column 8, lines 45-50 and column 7, lines 48-64); *to a corresponding set of known valid digest values* (MAC fields, col. 6, lines 59-65), (see column 8, lines 45-57). As interpreted by the Examiner, **Ansell et al** discloses allowing access to a smaller number of times of playback (see column 11, lines 26-38) or allowing access to a selected track of SPT (see column 13, lines 11-15 and column 9, lines 5-13), which meets the recitation of a smaller functionally equivalent version than the original version. **Ansell et al** further discloses allowing access to an encrypted compression version (see column 8, lines 63-67) which is smaller than the original based on the matching of digests values to a subset of verification data (see column 8, lines 45-67) that meets the recitation of *controlling access to a functionally equivalent version of the given content which is smaller than the original version if the digests values match a subset of verification data* (see also column 5, lines 1-18); access to a compressed version which is smaller than the original such as an MP3 format is very well known in the art as disclosed in the background of **Ansell et al** (see column 1, lines 12-20) the invention can also be used to acquire music products from the Internet (see column 13, line 62 through column 14, line

12), therefore, as shown above allowing access to "smaller than the original version" is disclosed. **Ansell et al.** teaches binding content and media identification by generating a digest value for each of a plurality or set of blocks of data (keys and component keys) retrieved from a storage medium but is silent about the word randomly when teaches retrieving data. However, **Herzberg et al.** in an analogous art teaches protecting multimedia title or program (content) including binding content with media identification (column 6, lines 47-64) by *randomly retrieving a plurality of blocks of data from a removable medium* (CD ROM) to determine if the content is valid (see column 7, lines 11-18 and column 5, lines 58-60 and column 2, lines 9-14), the random selection helps reduce the possibility of forgery, and processing time, (see column 12, lines 26-32). **Herzberg et al** further discloses calculating a digest value for each of the plurality of randomly retrieved blocks of data (see column 2, lines 17-21) *comparing digest values* (hash values) *to a corresponding set of known valid digest values* (hash values) *and controlling access if the calculated digests values* (hash values) *match a subset of associated verification digest values* (hash values) (see column 2, lines 20-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Ansell et al** with **Herzberg et al** to include the features of randomly retrieving/selecting when retrieving/selecting a plurality or set of blocks of data to be validated by generating a hash (digest) value for each of the plurality of randomly retrieved blocks of data and comparing hash values (digest) of the plurality or set of data portions of the content as taught by **Herzberg et al** above in order to more efficiently validate the multimedia program because the random selection helps reduce the possibility of forgery and processing time as the checking may be based on only portion of the data (see **Herzberg et al**, column 6, lines 18-39 and column

12, lines 26-32). This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestions provided above by **Herzberg et al.** so as to more efficiently validate the multimedia program to reduce the possibility of forgery, the motivation to do so is provided by Herzberg who teaches the advantage of checking only a selected portion of the data to be validated rather than checking all of the data *(see column 6, lines 18-34)* in order to minimize the required processing time, *(column 12, lines 26-32).* As indicated above, checking a small portion of data could be exposed to forgery, thus the invention as taught by Herzberg provides a degree of randomness, "by randomly selecting the portion of data to be validated, the possibility of forgery can be greatly reduced" (see column 6, lines 18-34).

As per claim 59, the combination of **Ansell et al.** and **Herzberg et al** discloses *wherein the verification module is adapted to control access to related material if the calculated digest values match a subset of the known valid digest values* (see **Ansell et al**, column 8, lines 45-67 for allowing access to a decrypted version of the key that meets the recitation of related material); (see also **Ansell et al**, column 5, lines 1-18 for allowing access to SPT 116 from tracks 112 or different forms of data (images, video, computer software) that also meets the recitation of related material).

As per claim 61, the combined references above disclose the claimed system of claim 58. **Ansell et al** discloses a computer system 100, connected through the Internet or Intranet network 170, comprising memory for storing shared data, the computer system 100 includes

player 110 and player 150, (see figure 1) (see also claims 20-21), the computer system 100 meets the recitation of server. Since the computer system 100 includes player 110 and player 150, (see figure 1), the verification module and SPT 116 containing corresponding set of known valid digest values, (see column 6, lines 50-65) as disclosed in claim 58 are therefore located in computer system 100 (server). **Ansell et al** discloses other player such as player 150B, figure 5 (*reading device*) coupled to the computer system (server).

(10) Response to Argument

Appellant's statements on the grounds of rejection are not correct. The issues raised by appellant were fully responded under the grounds of rejection. On page 8, second paragraph of the appellant brief, appellant argues that Ansell et al, hereafter Ansell does not disclose a computer readable medium. Appellant states, "*the Office appears to forget that the storage key 504A and its individual component keys are not retrieved "from a computer-readable media". Instead, they are integrated into the player itself, each particular storage key being unique to its corresponding player (e.g., see Abstract, Column 6 (lines 34-40)). In fact, each player's key is difficult to change, "typically requiring physical deconstruction" of the portable player. (see Column 6 (line 40))*." Examiner recognizes this specific citation in Ansell. However, Appellant misinterprets the abstract of Ansell. In the abstract, Ansell makes reference to two embodiments: the binding may be performed by software using digital signature (digest or hash) or the binding may be performed by hardware embedded in circuitry (see portions of abstract below):

"The SPT is bound to a particular storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed. The SPT can also be bound to the storage medium by embedding cryptographic logic

circuitry, e.g., integrate circuitry, in the packaging of the storage medium."

In addition, the citations provided in the rejection above clearly shows that keys are stored in storage medium accessible by the players. In fact, *in the original specification page 18, lines 3-4, medium* is referred to as *device that can store data that is accessible by a computer.* The keys in Ansell are accessible by computer systems as they can be shared or exchanged between players and cryptographically signed (figure 8B, steps 818 and 868, column 10, lines 43-48), therefore they are not binded by hardware, but by cryptographic signature (software). Appellant even admits on page 14 of the brief "Ansell's very operation depends on selecting keys from the storage medium". Appellant argues on page 9, lines 2-3 of the appellant brief that Ansell cannot possibly disclose ***if the digest values match*** *a subset of the verification data.* Examiner respectfully disagrees. It appears that appellant is arguing the plural form of the limitation in the claim. Note that figures 2 and 5 show that only one block of data is selected and only if additional verification is required that another block is selected. Also the citations provided by Applicant clearly shows a block is selected and a digest is performed and the result is compared to the known verification data. (see for instance page 13, lines 11-17). The independent claims as claimed do not require a plurality of blocks of data to be retrieved at one time as argued by Applicant with respect to Ansell. Appellant argues that Ansell does not disclose "smaller than the original version" as that term is used and understood in the context of the subject application (page 6, lines 10-15). Appellant is reminded that limitations in the specification cannot be read into the claim. In addition, the specification mentions examples such as "smaller than the original version" can be accomplished through compression or by omitting parts of data. Ansell discloses,

"In step 1306 (FIG. 13), player logic 502A (FIG. 5) decrypts the content of SPT 116 using the decrypted media master key. After step 1306 (FIG. 13), the content of SPT 116 is un-encrypted and is available for decompression and playback by player logic 502A. Decompression and playback of the un-encrypted content is conventional." (column 13, lines 27-32).

Therefore, the compressed content of the SPT is a version "smaller than the original version" (see also column 7, lines 9-10).

Appellant argues that Herzberg et al hereafter Herzberg teaches "**pre-selecting sections**" and randomly selecting data objects from the **pre-selected sections** of the program. The claims do not require that the data are not pre-selected. The claims merely recite "randomly retrieving plurality of blocks of data" which is broader than what is argued by Appellant. Herzberg, column 14, lines 63-64 explicitly recites and claims "randomly selecting a plurality of sections from within the program".

Appellant's showing of improper motivation on page 14, second paragraph of the brief is not logical. Appellant mentions that if Ansell's data blocks were retrieved randomly as suggested by the Office, the keys would rarely if ever be available to form digests. Ansell discloses, however, that the keys are provided to the player, therefore they would be available and discloses forming a digest for each one of the keys.

"player logic 502A forms respective digests of each component key of read-only key 504A and each of keys 506A1-4 using the same algorithm employed by player 110 (FIG. 1) in step 606 (FIG. 6)" (column 8, lines 46-48).

Randomly retrieving each data and forming a digest of each randomly retrieved data would be more beneficial than forming a digest for all the data in the medium as disclosed in Herzberg and explained in the rejection above.

Regarding the dependent claims, the issue raised by appellant was fully responded under the grounds of rejection as shown above. Since Appellant provides the same arguments in claims 52-53 as in claim 45 although the claims do not disclose the same, the issue raised by appellant can be found either in claim 45 above or in the rejection of claims 52-53 in the last final rejection.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

CC

Carl Colin

December 4, 2006

Conferees:

Eddie Lee

Nasser Moazzami

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052